



# Data protection in outsourcing transactions: the UK experience

Andrew Dunlop and Uwe Nimscheck  
Burgess Salmon LLP

[www.practicallaw.com/5-506-1203](http://www.practicallaw.com/5-506-1203)

Outsourcing often requires the transfer of personal data held by the outsourcing company (or client) about individuals to the outsourcing provider. Examples include the client's customer details in a financial services outsourcing project or the client's employee data in payroll outsourcing.

Protection of personal data in the European Economic Area (the EEA, which includes the EU, Iceland, Liechtenstein and Norway) is based on Directive 95/46/EC on data protection (Data Protection Directive). The Data Protection Directive has been implemented in the UK by the Data Protection Act 1998 (DPA), which is the main data protection legislation covering the UK. The ICO (Information Commissioner's Office) is responsible for enforcing the DPA in the UK.

This article outlines some key issues companies should consider regarding the processing of personal information in UK outsourcing transactions. In particular it explains:

- The principles that the DPA contains concerning the processing of personal data (*see box, The DPA's data protection principles*).
- What types of data the DPA covers.
- The key rights that the DPA gives to data subjects.
- The consequences for companies of breaching the DPA.
- The key issues that arise in outsourcing transactions as a result of the DPA's requirements.

## THE DPA: TYPES OF DATA COVERED

The DPA covers personal data, which is data relating to a living individual (called the data subject) who can be identified from that data, or from that data together with other information that is in the possession of, or is likely to come into the possession of, the data controller. In a business context, this includes information relating to employees, customers and suppliers. Because of the wide definition of personal data, areas such as CCTV images or telecommunications can also constitute personal data.

The DPA also identifies "sensitive personal data", which is personal data relating to:

- Racial or ethnic origin.
- Political opinions.
- Religious beliefs or beliefs of a similar nature.
- Trade union membership.
- Physical or mental health or condition.
- Sexual life.
- Commission or alleged commission of any offence, or proceedings for any offence, or sentence of court.

The list contained in the DPA is exhaustive. Financial information relating to an individual does not constitute sensitive personal information. The obligations relating to sensitive personal information are more onerous than those relating to personal data and are outside the scope of this article (for more information, see *Data Protection: UK (England and Wales)*).

Because of the often onerous obligations imposed by the DPA, companies should always consider whether it is possible to move themselves outside the realm of the DPA by anonymising data so that it no longer constitutes personal data.

## RIGHTS OF DATA SUBJECTS

The DPA gives comprehensive rights to data subjects in relation to their data. In relation to outsourcing transactions, the most important rights include:

- Access to personal data.
- Prevention of certain kinds of processing.
- By way of court order, rectification, blocking, deletion and destruction.

These rights are generally enforceable against the outsourcing company as data controller rather than against the data processor. Where the outsourcing provider handles personal data on its client's behalf, the client as the data controller should include appropriate provisions in the outsourcing contract to ensure the outsourcing provider's collaboration. This includes obligations to:

- Amend, transfer or delete the data as requested by the client.
- Notify the client of data access requests or complaints that it receives in relation to the client's data and provide the client with full co-operation in relation to such requests or complaints.

However, the client should ensure that it has sole conduct of such requests by preventing the outsourcing provider from responding directly to the data subject unless instructed to do so by the client.

The outsourcing company should also include an obligation on the data processor to be notified immediately if any of the following occur:

- Data gets accidentally deleted or corrupted.
- Data becomes lost.
- The outsourcing provider becomes aware that the data is processed unlawfully.

This is to ensure that the client can take the necessary steps to address the issue, including notification to the ICO and/or the data subjects if required.



## CONSEQUENCES OF BREACH

Compliance with DPA obligations is key, not only because of the direct impact of enforcement actions, but also because of the potential damage to reputation.

There are a number of ways in which the ICO enforces the DPA, including criminal prosecution, non-criminal prosecution and audit. The ICO also has the power to issue monetary penalty notices of up to GB£500,000 (as at 1 February 2011, US\$1 was about GB£0.6) on the data controller for serious or deliberate breaches of the DPA. Enforcement will be against the data controller.

Failure to comply with Principles 7 or 8 of the DPA (see box, *The DPA's data protection principles*) is normally addressed by:

- Serving information notices that require the data controller to provide information about its processing operations.
- Issuing undertakings in which the data controller commits itself to certain actions or stops certain activities to ensure compliance with the DPA.
- Serving enforcement notices and “stop now” orders, which are most likely to be used where there has been systematic or repeated non-compliance with the DPA or undertakings.

Failure to comply with an enforcement notice is a criminal offence, which may result in court action. Outsourcing companies should also not underestimate the impact of undertakings issued by the ICO, as the actions required might severely disrupt their business processes. Undertakings and enforcement notices are also published on the ICO's website and frequently reported in the press, which is likely to cause damage to the reputation of the company.

## KEY ISSUES TO CONSIDER

Key issues in outsourcing transactions often arise as a result of the obligations imposed by the Principles 1, 7 and 8 of the DPA (see box, *The DPA's data protection principles*). They centre on the following three areas:

- **Establishing responsibilities.** The data controller needs to be ascertained, based on the requirement that processing of the data by the outsourcing provider be fair and lawful (*Principle 1*).
- **Imposing contractual obligations.** The data controller needs to ensure that appropriate technical and organisational measures are in place to ensure security of the data (*Principle 7*).
- **Complying with the export ban.** Appropriate measures need to be put in place to ensure that any export of personal data outside the EEA affords adequate protection to the individual (*Principle 8*).

In addition, the company needs to ensure that individuals are given access rights to their personal data as granted by the DPA. This often requires the collaboration of the outsourcing provider to the extent that it holds such data.

The DPA exists in a larger framework of legislation such as the Freedom of Information Act 2000, the Regulation of Investigatory Powers Act 2000 and industry specific legislation such as the Financial Services and Market Act 2000 (for financial services companies) and Privacy and Electronic Communications (EC Directive) Regulations 2003 (E-Privacy Regulations) for communications companies. The requirements of this legislation also need to be considered (see box, *UK legislative framework*).

## Establishing responsibilities

The DPA distinguishes between data controllers and data processors. The distinction is important, because the obligations under the DPA are imposed on the data controller. No obligations are imposed on the data processor in relation to the data controller's data (even though, of course, a UK-based data processor has obligations in relation to its own personal data, for example, its own payroll). As a result, the data controller is responsible for complying with the DPA and is liable for any breaches.

A data controller determines the purpose and means of the processing, while a data processor processes data on behalf of the data controller. The data processor may have some discretion in determining the technical and organisational means of the processing. In practice, the distinction between data controller and data processor is not always clear. The Article 29 Working Party (which is composed of representatives of the national data protection authorities and is an independent advisory body to the European Commission on data protection matters) has recently published an opinion seeking to clarify the concepts (see [http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/c\\_2010\\_593/c\\_2010\\_0593\\_en.doc](http://ec.europa.eu/justice/policies/privacy/docs/modelcontracts/c_2010_593/c_2010_0593_en.doc)).

In a typical outsourcing transaction, the outsourcing provider processes data on behalf of the client, so the client would be assumed to be the data controller and the outsourcing provider the data processor. However, in some outsourcing transactions the parties may maintain a joint database and make independent use of the data (for example, for separate marketing operations) and in this case both the client and the outsourcing provider would be considered data controller in relation to the data.

Outsourcing contracts frequently contain a statement defining the client as the data controller and the outsourcing provider as the data processor, but their status under the DPA is largely a question of fact rather than of the intention of the parties as set out in the contract.

The first principle of the DPA requires personal data to be processed fairly and lawfully and in accordance with the conditions set out in the Schedules to the DPA. The conditions relevant for personal data (other than sensitive personal data) are set out in Schedule 2 to the DPA. Schedule 2 lists six conditions under which data is processed lawfully and the data controller has to rely on one or more of these criteria to be met for the data to be lawfully processed by the data processor. In the context of outsourcing transactions, clients frequently rely on condition six, which allows processing necessary for the purposes of legitimate interests pursued by the data controller.

## Imposing contractual obligations

As it is the client's (as data controller) rather than the outsourcing provider's (as the data processor) responsibility to comply with the DPA, in relation to the outsourcing company's data, it must ensure that it imposes all necessary obligations in relation to data protection on the outsourcing provider through a contract. The relationship between controller and processor is reflected in the seventh principle of the DPA, which requires the data controller, where it appoints a data processor to:

- Carry out the processing under a contract made or evidenced in writing.
- Require the data processor to act only on instructions from the data processor.



- Require the data processor to comply with obligations equivalent to those imposed on the data controller by the seventh principle.

The scope of Principle 7 is far wider than the controller-processor relationship. It requires the data controller to take appropriate security measures (both technical and organisational) to ensure an appropriate level of security of personal data, regardless of whether data is processed by the data controller itself or the data processor. What constitutes appropriate security measures depends on:

- The available technology.
- The cost of implementing such technology.
- The nature of the data.
- The harm that might result from a breach of security.

Breaches of security could include not only unauthorised access or unlawful processing, but also accidental loss or damage to personal data. As a result, appropriate security measures should:

- Include appropriate software and hardware measures such as virus protection, firewalls and encryption.
- Extend to general security measures such as storing personal data in a safe building with access control, and appropriate vetting and authentication of personnel with access to personal data.

If the outsourcing company engages an outsourcing provider as data processor, Principle 7 requires that it ensure that the data processor also has appropriate security measures in place.

This obligation extends beyond merely including such obligations into the contract: as the client will be held accountable for the data processor's breaches, it also needs to ensure that the data processor has actually implemented and continues to keep in place the requisite security measures. Necessary steps might include requiring the outsourcing provider to provide documentary evidence of the implemented measures and auditing these measures on site, not only before the contract commences, but also during the term of the outsourcing contract on an ongoing basis.

Most outsourcing providers are familiar with their client's requirements in this respect and will already have appropriate documentation detailing their security measures, but they might be more reluctant, for reasons of confidentiality, to grant to the client (or its auditors) auditing access to its premises.

The outsourcing contract should also contain provisions if the data processor is allowed to transfer the data to sub-processors.

### Complying with the export ban

The export of personal data to a data processor located in another EEA country does not represent particular issues other than those set out above. However, outsourcing providers frequently transfer personal data to locations outside the EEA, for example, a data processing facility or call centre in Asia. This is often part of the business model of the outsourcing provider and is attractive to it as it gains an economic benefit from the low labour cost location. However, any increased risk from a data protection point of view rests with the outsourcing provider's client as the data controller. As a result, the client usually seeks to obtain a fair share of the economic benefit and to mitigate its own risks in relation to data security.

Principle 8 contains a ban on exporting personal data to countries and territories outside the EEA unless an adequate level of protection is ensured. The Commission has identified a number of countries that it considers to offer adequate levels of data protection similar to those in the EEA. The list includes only a limited number of countries including Andorra, Argentina, Canada (subject to conditions), Jersey, Guernsey, the Isle of Man, Switzerland and Israel, but not, for example, the US.

Where the Commission has not made a finding of adequacy for a certain country, the client as data exporter may make its own assessment of adequacy using a number of general and legal adequacy criteria set in out in Part II of Schedule 1 to the DPA. Few data exporters rely on this approach because of the inherent risk that, if security issues arise with the exported data, the ICO might not agree with the data exporter's assessment of adequacy and find the data exporter in breach of Principle 8. If a data exporter follows this approach, it should at a minimum keep some written documentation demonstrating that its assessment of adequacy was the outcome of a structured decision-making process that considered the guiding factors set out in the DPA.

When assessing the data export, clients should also consider the impact of local legislation on the data processor, for example, the impact the US Patriot Act may have on disclosure requirements by US data processors.

Rather than making their own findings of adequacy, data exporters frequently rely on one of a number of exemptions to the export ban that are set out in Schedule 4 to the DPA. In practice, outsourcing companies are likely to rely on one of the following two exemptions:

- The model contract clauses.
- The Safe Harbor scheme.

There are also some other options available to ensure that data transfers occur in accordance with the DPA.

**Model contract clauses.** The Commission has issued decisions that approve a set of model contractual clauses so that, where transfers are made using these model clauses, adequacy under Principle 8 of the DPA is ensured.

Different sets of model clauses have been approved to cover the export to data controllers and to data processors. The latter is the more usual situation in outsourcing transactions, but the data exporter must consider carefully whether the outsourcing provider is a data controller or data processor to ensure the right set of model clauses is used.

The model clauses are short form contracts that impose obligations on the data exporter and the data importer to ensure that the data transfer complies with the DPA. They also confer rights on the data subject to enforce its rights directly against the data exporter and the data importer. One advantage of using the model clauses is that they ensure a transfer complies not only with Principle 8 of the DPA but also with Principle 7 (*see above, Imposing contractual obligations*).

The model clauses can be used on a stand-alone basis or attached to larger contracts. To ensure their status as approved by the Commission, they must be used "as is" and cannot be amended by the parties. However, additional clauses containing commercial details can be added by the parties to the extent that they do not conflict with or negate the model clauses.



In outsourcing transactions, the situation frequently arises that the outsourcing provider as data processor in turn sub-contracts the processing of personal data to a sub-processor. Two scenarios must be considered:

- The outsourcing company as data controller exports to a data processor outside the EEA, which in turn transfers to a sub-processor outside the EEA.
- The outsourcing company as data controller transfers to a data processor within the EEA, which in turn exports to a sub-processor outside the EEA.

In relation to the first scenario, previous versions of the model clauses did not contemplate the data processor transferring the data to a sub-processor. However, the current version of the controller-processor model clauses, approved by the Commission in 2010 (2010/87/EU), now allows the data processor to outsource to a sub-processor as contemplated in the first scenario, provided appropriate contractual obligations are imposed on the sub-processor. However, there are currently no model clauses setting out the contractual obligations that the processor is to impose on the sub-processor. Additional complexity arises in the second scenario, where the outsourcing provider (the processor) is located in the EEA and the export of the data outside the EEA is effected between the processor and the sub-processor (rather than between the data controller and processor, as in the first scenario). The Article 29 Working Party has recently confirmed its view that the model clauses do not apply in these circumstances and cannot be used if data is transferred from an EEA-based controller to an EEA-based processor and then exported to a non-EEA-based sub-processor (see *FAQ to Decision 2010/87/EU at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp176_en.pdf)*).

The Working Party is currently considering the adoption of specific model clauses to cover this scenario. Meanwhile, it has identified three options:

- A direct contract between the EEA-based controller and non-EEA-based sub-processors, under which the non-EEA-based sub-processor signs the model clauses as data importer (processor) rather than sub-processor.
- A clear mandate from the EEA-based data controller to the EEA-based processor to use model clauses 2010/87/EU in its name and on its behalf.
- Ad hoc contracts containing the principles and safeguards set out in the model clauses.

**Safe Harbor scheme.** Another option for the export of personal data to companies based in the US is the Safe Harbor scheme. Safe Harbor is a self-certification scheme that has been set up by the US Department of Commerce and is based on seven principles broadly equivalent to the requirements of the DPA. It is recognised by the Commission as a standard of data protection that is consistent with the requirements of Principle 8 and allows UK companies to export personal data in accordance with the DPA to participating US organisations.

The scheme is open to US organisations subject to the jurisdiction of the Federal Trade Commission (FTC) or the Department of Transportation (DoT), which excludes certain organisations such as financial institutions and telecoms carriers. Generally, take-up of the scheme has been slower than anticipated, although some large organisations such as Apple and Microsoft are registered. The US Department of Commerce maintains a list on their website of companies that have registered with the scheme (see <https://safeharbor.export.gov/list.aspx>).

**Other options.** Binding corporate rules are sometimes used by large multinational organisations to ensure that intra-group transfers are conducted in accordance with the DPA. They consist of a set of company-specific rules that must be submitted for approval by the Commissioner. As they specifically apply to company-internal transfers, they are generally not suitable to arm's-length outsourcing transactions.

Another option is to rely on the data subject's consent to export its personal data outside the EEA. Although this option may initially be appealing, it is difficult to rely on in practice, as pointed out by the Article 29 Working Party in its working document WP 114. As set out in the Data Protection Directive, the data subject's consent must be:

- Given freely.
- Specific.
- An informed indication of the data subject's wishes.

It is conceivable that a data subject could give such consent for a specific transaction, although it is unclear if an employee's consent to the export of his human resources data would be "freely given", given the often unequal balance of power between employer and employee.

More importantly though, it is difficult for a data subject to give his informed consent for a number of transactions in advance, as this would require him to be aware of the specific circumstances of future transactions, including for example, the specific risks associated with the transfer of data to a certain country for which no finding of adequacy exists.

### THE DPA'S DATA PROTECTION PRINCIPLES

The Data Protection Act 1998 (DPA) requires the processing of personal data in accordance with eight data protection principles:

- **Principle 1.** Personal data must be processed fairly and lawfully and in accordance with the conditions set out in the Schedules to the DPA.
- **Principle 2.** Personal data must be obtained and processed only for one or more specified and lawful purposes.
- **Principle 3.** Personal data must be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- **Principle 4.** Personal data must be accurate and, where necessary, kept up to date.
- **Principle 5.** Personal data must not be kept for longer than is necessary for the purpose for which it is processed.
- **Principle 6.** Personal data must be processed in accordance with the rights of data subjects under the DPA.
- **Principle 7.** Personal data must be processed with appropriate technical and organisational measures taken against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- **Principle 8.** Personal data must not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection.

Outsourcing transactions must ensure that they will not lead to the breach of any of the above principles.



## UK LEGISLATIVE FRAMEWORK

Outsourcing companies should be aware that the Data Protection Act 1998 (DPA) forms part of a larger framework of UK legislation seeking to protect the individual's interests in its personal data.

The Freedom of Information Act 2000 (FOIA) gives a qualified right of access to any information held by public authorities. If the company is subject to FOIA, it may need the data processor's collaboration in relation to FOIA requests and appropriate obligations should be included in the contract.

The Regulation of Investigatory Powers Act 2000 (RIPA) covers public and private telecommunications systems. Unless authorised by the relevant Secretary of State, it prohibits interception of communications over public telecommunications systems and, with certain exceptions, also over private telecommunications systems. This may impact on outsourcing contracts covering telecommunications systems in two main ways:

- Personal data may be lawfully intercepted under authorisation by the Secretary of State when communicated to the outsourcing provider.

- Where telecommunications are lawfully intercepted within a private communications system (for example, recording of conversations for evidential purposes in a transactional call centre environment operated by an outsourcing provider), the outsourcing company needs to ensure that both itself and the outsourcing provider are acting in a lawful purpose as set out in the Lawful Business Practice (Interception of Communications) Regulations 2000.

Clients subject to the Financial Services and Markets Act 2000 (FSMA) wishing to outsource also have to comply with specific additional obligations set out, for example, in the Financial Services Authority Handbook of Rules and Guidance and in Directive 2004/39/EC on markets in financial instruments (MiFID).

Outsourcing transactions conducted by providers of public communication systems are also subject to industry specific regulations, such as the E-Privacy Regulations, which complement the DPA (and as such are without prejudice to any obligations arising under the DPA). The E-Privacy Regulations require appropriate technical and organisational measures to safeguard the security of the service, which also extend to the outsourcing provider.

## CONTRIBUTOR DETAILS



### ANDREW DUNLOP

*Burges Salmon LLP*

T +44 117 902 2786

F +44 117 378 6112

E [andrew.dunlop@burges-salmon.com](mailto:andrew.dunlop@burges-salmon.com)

W [www.burges-salmon.com](http://www.burges-salmon.com)



### UWE NIMSCHECK

*Burges Salmon LLP*

T +44 117 902 7258

F +44 117 378 6479

E [uwe.nimscheck@burges-salmon.com](mailto:uwe.nimscheck@burges-salmon.com)

W [www.burges-salmon.com](http://www.burges-salmon.com)

**Qualified.** Scotland, 1988; England and Wales, 1991

**Areas of practice.** Commercial transactions, particularly outsourcings and joint ventures.

#### Recent transactions

- Advising international corporate (food and beverages) on its outsourced cloud computing arrangements covering 44,000 employees in Europe and Africa.
- Advising FTSE 100 (financial) on the renegotiation of its worldwide telecommunications outsourcing.
- Advising FTSE 150 (defence) on its new global ERP arrangements.
- Advising FTSE 100 (energy) on its global outsourced IT arrangements.
- Advising FTSE 150 (technology) on compliance issues arising under data protection, freedom of information, regulation of investigatory powers and human rights legislation.

**Qualified.** England and Wales, 2008

**Areas of practice.** Data protection; IT outsourcing; software licensing; intellectual property law.

#### Recent transactions

- Advising two UK financial services companies on the outsourcing of back-office functions to non-EU jurisdictions including the US and India.
- Advising one of Europe's largest bottling companies on the outsourcing of its data centre services covering over 30,000 employees in 28 countries.
- Advising a European marketing company on data protection issues in relation to its UK marketing campaigns.
- Advising leading offshore legal and IP services outsourcing companies on UK data protection issues.